2766

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE PATENT APPLICATION OF: **Howard et al** File No: **79-4 US**

Serial No: **09/244,203** Group: **2766**

Filed: **February 4, 1999** Examiner: **Unknown**

For: **SYSTEM AND METHOD FOR CIPHERING DATA**

The Commissioner of Patents and Trademarks
Washington, D.C., 20231, U.S.A.

May 25, 1999

Dear Sir:

Enclosed please find a certified copy of the priority document in support of the above-identified patent application.

Respectfully,

N. Teitelbaum
Reg. No. 38,793

Neil Teitelbaum and Associates
834 Colonel By Drive
Ottawa, Ontario
Canada, K1S 5C4

Tel (613) 730-0510
Fax (613) 730-0536
Email: neil@patents.org

OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

OIPE JC
MAY 26 1999
PATENT & TRADEMARK OFFICE

Bureau canadien des brevets

Canadian Patent Office

Certification

La présente atteste que les documents ci-joints, dont la liste figure ci-dessous, sont des copies authentiques des documents déposés au Bureau des brevets.

Certification

This is to certify that the documents attached hereto and identified below are true copies of the documents on file in the Patent Office.

RECEIVED
MAY 28 1999
Group 2700

Specification and Drawings, as originally filed, with Application for Patent Serial No: **2,228,687**, on February 4, 1998, by **BRETT HOWARD, PAUL KIERSTEAD, GABOR SOLYMAR, ANDREW ROBINSON, AND ROY PEREIRA**, for "Secured Virtual Private Networks".

S. Gregoire

Agent certificateur / Certifying Officer

February 15, 1999

Date

Abstract of the Disclosure

A method and system for securing a communication network using a publicly accessible security medium is disclosed. According to the method, a secured virtual private network is maintained allowing for a variety of different secure network topologies.

Secured Virtual Private Network

Field of the Invention

This invention relates generally to communications networks and more particular to a secured virtual private network (SVPN).

Background of the Invention

Computer security is fast becoming an important issue. With the proliferation of computers and computer networks into all aspects of business and daily life - financial, medical, education, government, and communications - the concern over secure file access is growing. One method of providing security from unauthorized access to files is by implementing encryption and cipher techniques. These techniques convert data into other corresponding data forms in a fashion that is reversible. Once encrypted, the data is unintelligible unless first decrypted. RSA, DES, PGP, and CAST are known encryption techniques that are currently believed to provide sufficient security for computer communications and files.

Historically, secure networks were achieved by preventing access to data within the network by those outside the network. Networks were formed of a number of computers interconnected by cables. No access to the network was permitted save through the use of one of the interconnected computers. In order to use these computers, it was necessary to be physically located within a building housing the network.

With the proliferation of modems, it became clear that remote access is a powerful tool. In order to provide remote access to network data, dial-up servers were maintained in communication with a public communication network such as a phone network. An individual wishing access to the network, connects to the dial-up server with a computer equipped with a modem or another appropriate communication device, logs into the network, and is then provided access to the network. In this fashion, network data is only

communicated over communication channels within the physical network and over dedicated dial up connections. This was commonly viewed as less secure than the physically isolated computer network, but due to its advantages became common place.

With the proliferation of the Internet and Internet based communications, a need has arisen to provide secure communications via an unsecured public network. Encryption is commonly used to provide this security. For example, PGP (pretty good privacy) is an available encryption software product which implements a private-public key encryption system. Files are encrypted prior to transmission and then decrypted upon reception. The communicated file is secured by the encryption and is as secure as the encryption process used. For occasional file transfers, PGP and similar software products are excellent. Unfortunately, they are not well suited to network access via the public network.

In order to provide SVPNs, IPSEC (Internet Protocol Security) protocol suite was developed. IPSEC is a set of industry-standard extensions to the Internet Protocol (IP) that add security services. The suite contains protocols for an authentication header (AH) assuring data integrity, an encapsulating security payload (ESP) format ensuring data privacy, and a key management and exchange system (ISAKMP / Oakley). These industry-standard protocols allow for development and implementation of SVPNs.

Unfortunately, many commonly available network features are not available using these protocols. Also, flexibility is often compromised to ensure security. It would be advantageous to provide a high degree of flexibility, a broad range of network features, and a high level of security.

Object of the Invention

It is an object of this invention to provide an SVPN having increased flexibility and increased features over those currently available using the IPSEC protocol suite.

Brief Description of the Drawings

An exemplary embodiment of the invention will now be discussed in conjunction with the attached drawings in which:

Fig. D1 is a simplified schematic diagram of an SVPN;

Fig. D2 is a simplified flow diagram of a method of tunneling from a secured workstation through an unsecured communication channel to another secured workstation;

Fig. D3 is a simplified schematic diagram of the certificate database system for an SVPN according to the invention;

Fig. D4 is a simplified flow diagram of a method of authenticating a certificate in order to secure a communicaiton according to the invention;

Fig. D5 is a simplified flow diagram of a method of implementing policies according to the invention;

Fig. D6 is a simplified block diagram of a system architecture comprising a network virtual adapter according to the invention; and,

Fig. D7 is a schematic diagram of a network comprising three sub-networks and an unsecured communication medium between two of the sub-networks.

Detailed Description

Appendix A attached hereto provides information relating to a family of products implementing some of the inventions described herein. Appendix A also contains background information and definitions.

Commonly when a user logs into a network, the user is provided access to the network according to established rules. For users physically located within a secure environment, these access restrictions prevent dissemination of sensitive information. For example, access to human resource data is often restricted. For users physically located outside the secure environment, these access restrictions prevent hacking – illegal access – from presenting a significant threat to data integrity and security.

Referring to Fig. D1, a secured virtual private network (SVPN) is shown. An unsecured communication medium 1 in the form of the Internet forms a communication backbone for the network and allows for communication between different geographical locations. In communication with the unsecured communication medium 1 are a variety of unsecured and secured systems (not shown). The SVPN operates across this communication medium providing secure communication through the medium 1 and transparent network operations. A secured network 3 is separated from the unsecured communication medium by a gateway 5. The gateway 5 acts to secure communications with other gateways and with workstations 7a provided with appropriate software. Workstations 7b located within secured networks 3 communicate with the network absent gateway security. The secured network also comprises a file server 7c and peripheral devices 7d.

Referring to Fig. D2, a simplified flow diagram of a method of communicating between workstations on different secured network segments is shown. When a message from a workstation 7b to another workstation separated from the workstation 7b by the unsecured communication medium 1 is sent, the message is packaged according to the secured network protocol and transmitted via the secured network. When the message is received by the gateway, it is secured and packaged for transmission over the Internet. Preparation of information for transmission via the Internet is well known. The secured message with unsecured Internet protocol and address information is then transmitted via the Internet to a destination gateway forming part of a second secured network. The destination gateway receives the message and extracts it from the Internet protocol and address information and then extracts the message from the secured message. The resulting unsecured message has network information and addressing information for the secured network. When the receiving gateway forms part of a second network using a different network communication protocol, the gateway or a communication server translates the message to an appropriate format for the receiving network. The message is then transmitted via the second secured network to the destination workstation. Using the

method of Fig. D2, communication between two workstations separated by the unsecured communication medium 1 is transparent to a user.

Referring to Fig. D3, a certificate database system is shown. An x500 database 31 interacts with a certificate authority 33. The certificate authority 33 provides for certificate authentication, certificate distribution, and certificate creation. The database 31 provides for certificate storage and allows for storage of a sufficient number of certificates. Of course, when a network is so large that more certificates are necessary, other larger certificate databases are used or, alternatively, a plurality of different certificate databases are used. Hereinbelow, a method of using a plurality of certificate databases in a secure fashion is described. A server 35 provides network communications for the certificate authority 33 and the database 31. Certificate authentication and retrieval is a process requested by gateways because it relates to secure communication via the unsecured communication medium 1.

Authentication of systems using a certificate is well known. According to a method of performing authentication as shown in Fig. D4, a secured certificate is transferred to another system for authentication. Once authenticated as a correct certificate, communication is initiated. The communication is verified to be with a system providing an authenticated certificate. When the certificate contains data, the data is usable once the certificate is authenticated because the data is then known to accurately reflect data within the certificate database. For example, a certificate containing an encryption key is authenticated prior to using said key in communications. This ensures use of correct encryption keys and prevents transmission of information – even encrypted information – to incorrect destinations.

Referring again to Fig. D3, a director system 37 in the form of a workstation communicates with the certificate database to provide attribute certificates and to direct retrieval and implementation of attribute certificates for network security. When attribute certificates are used, the gateways implement access security verification. Alternatively,

certificates are accessible to network resources that perform access security verification. Further alternatively, access security verification is performed at multiple locations in order to enhance overall security through redundant security checks.

When a director system 37 is installed within the SVPN certificates are used to define SVPN policies such as those relating to access. Optionally, other policies and policy types are implemented as well. Attribute certificates – a subset of certificates – are used to store information relating to users and policies relating thereto. Policies unrelated to specific users, are also supported.

Policy certificates serve similar functions to identification certificates and data certificates. A policy certificate comprises information relating to policies for implementation within a network. For example, an attribute certificate comprises information linking a user, a resource, and an access policy; the user is linked to the resource by the policy and when the user seeks access to the resource, the policy is enforced. Some examples of policies include read/write access, read-only access, write-only access, low priority access, access only through another specified resource, rerouting of access to another resource transparently, and so forth. Because the policies are stored in a separate database, complex policies are easily implemented using the system of the present invention. Though in this example the attribute certificate comprises information linking a user and a resource, attribute certificates exist for linking a group of users and one or more resources; for linking a single user and several resources; for a user; for a resource; and for other policies.

When a user seeks access to a resource, an appropriate attribute certificate is retrieved and authenticated. The authenticated certificate is then decoded and the policy contained therein is implemented. When the attribute certificate is not authenticated, access is denied or another attribute certificate is retrieved for authentication and implementation. Referring to Fig. D5, a simplified flow diagram of implementation of a resource access policy is shown. An access request is made for a resource. The attribute

certificate for the resource is retrieved, authenticated, and a policy contained therein is implemented. As shown, the policy indicates that remote users are not provided access to the resource and that access is further restricted to users in group A. In some instances when multiple policies are contained in separate attribute certificates, policies relating to interactions between policies become necessary. These are implemented for an entire network or, alternatively, on a resource by resource basis.

In the flow diagram of Fig. D5, when the request to the resource emanates from a workstation remote from the secured network or from an individual who is not a member of Group A access to the resource is denied. When an attribute certificate security system is implemented as part of a gateway 5, policies result in permitted communication or denied communication. More complicated implementations of certificate based policies for network security, require broader implementation at individual resources within the network. In an embodiment, only the gateway is provided with a policy based security system. This provides for a convenient and secure method of establishing access of individuals to the network. The enhanced security provided by attribute certificates is advantageous.

Many advantages to such a system exist. A central policy database is easily maintained allowing for modification of access and other policies without accessing individual network nodes and resources. When a network is distributed in several locations, such a policy database allows for centralized security. Also, by requiring all resources to retrieve attribute certificates from the certificate database 31 and authenticate attribute certificates, each resource policy is current and difficult to tamper with. These and other advantages will be evident from the remaining disclosure.

The use of attribute certificates allows for network partitioning. Network partitioning provides for a single physical network having several "virtual networks" existing thereon. For example when company A and company B share a same premise, they preferable share hardware in order to reduce costs. A single gateway and a single

firewall and a single certificate authority are used. By implementing attribute certificates to define access of employees of company A to resources of company A and access of employees of company B to resources of company B, two networks appear to be installed. Further, the use of attribute certificates allows for different levels of security at the gateway depending on the resource requested and different levels of firewall security for different individuals. When a resource is shared, the resource appears on both networks. This is practical for a doorway security system, a specialized printer, a scanning device, and so forth.

In one embodiment, only access to network resources is controlled so network partitioning is limited to providing or denying access to different resources to different individuals or groups.

Alternatively, when policy based security is implemented within resources themselves, a resource implements further policies once access to the resource is provided. For example, for a shared printer an attribute certificate requires accounting of a number of pages printed in a file accessible to company A, company B, or to both company A and company B. In essence, a secured network may comprise any number of autonomous and interworking networks. These networks may include unsecured communication media and remote network sites. Applications of network partitioning are numerous. Some of the applications are outlined in Appendix A.

An advantage of network partitioning (network segmentation) is achieved by network service providers who partition their networks in accordance with the invention. For example, an Internet service provider (ISP) provides service to several companies. When the services include gateway services, it is advantageous to implement the service for all clients with a small number of gateways. It is evident to those of skill in the art that implementing a set of gateways and a dedicated server for each client is costly and wasteful. Even when a company has multiple sites to connect via the ISP, it is advantageous to the ISP to maintain a single physical network. A client's "virtual

network" appears as a physical dedicated network to the client. Each virtual network is customized to a client's particular needs. The cost savings to the ISP are evident. The ISP also benefits from increased flexibility and convenience; reconfiguring networks and upgrading software are performed on a single physical network in order to accommodate all clients.

Commonly when using a remote access client, Internet access is provided in one of two fashions. First, Internet access is provided via the secured network wherein each Internet access request is routed to the physical secured network forming part of the SVPN. From there the request is sent out via an Internet translation server or another Internet server to the public network. Such a system is wasteful of network resources because the remote access client is already connected to the public network. Alternatively, the remote access client logs off of the network and logs onto the Internet, separately. When a workstation shown as 7a in Fig. D1 accesses a network remotely, neither of these solutions is convenient or efficient.

Referring to Fig. D6, a virtual network adapter is provided within the remote access client. In this way, the client system appears to have a connection to a public network such as the Internet and a second other connection to the SVPN. In reality, a single physical connection exists to the public network and requests to the public network are routed via a network virtual adapter through the TCP/IP protocol adapter to the public network. Alternatively, both network adapters provide data to the network directly; requests to the SVPN are routed through the network virtual adapter and converted to requests for transmission over the public network. According to the embodiment of Fig. D6, a person communicating from a remote location need not be encumbered by the firewall of the SVPN. Also, the SVPN need not accommodate extra Internet traffic which is artificially routed thereto via the internet. The additional convenience and functionality provided by such a virtual adapter or by a dual adapter configuration is therefore advantageous. Since a single physical network connection is used, when a dual adapter

configuration is implemented conflicts may arise between adapters. This is particularly of concern when implemented in a multitasking environment. Many methods of avoiding conflicts such as semaphores are known in the art of operating system design. These are applicable to the implementation of a dual adapter system. Of course, when the network adapter is a network virtual adapter, the TCP/IP protocol adapter prevents any conflicts or race conditions from occurring.

Another common problem encountered in the use of SVPN systems is that of security concerns for mobile users. For example, when using a cellular modem, an individual may desire increased security. When dialing up an ISP that is identical to that used by the company, performance may be the most significant concern. When using a slow system, performance is critical. When using a very fast state-of-the-art system security is more important. According to an embodiment of the invention, a profile is created containing data relating to a security level, a network adapter, tunneling information, and so forth. When accessing the SVPN, a profile is selected and those settings are used. Preferably, profile authorization occurs to ensure that a desired level of security is achieved for the SVPN and that network security is not compromised. Profile authorization is implemented using attribute certificates to indicate profile authorization policies. The profile is evaluated in dependence upon a series of criteria including communication medium, location of the mobile user, identity of the mobile user, and desired level of security for the profile. Preferably, some attribute certificates contain policies for resources requiring a confirmation of profile authorization.

Alternatively, a profile is created and attribute certificates relating to the profile are created and stored in the certificate database of the SVPN. Upon authenticating the certificate of the profile, the associated attribute certificates are retrieved and used as needed. Such a system, increases security without reducing the centralized control provided by an attribute certificate based system. In another embodiment, a profile is flexible. Different attribute certificates are retrieved depending on an actual execution of

the profile. For example, a country of origin of a communication, the communication medium, and an identity of the mobile user is determined and an appropriate set of attribute certificates - policies - are used.

SVPNs are often provided with management systems. Security of management systems is essential to maintain network security. Flexibility of management systems provides enhanced usability and improved turn-around for problem correction. Often, increased flexibility results in decreased security. Management systems are implemented in two common fashions – for use on a single system and for use anywhere on a network. When used on a single computer system, physical security is possible therefore providing a high level of security. When used on networks, problems can be addressed where and when located. It would be advantageous to provide a management system with enhanced security and significant flexibility. According to the invention, a management system is implemented wherein an integrity check is performed on each piece of network traffic for use in network management. Preferably, the integrity check is performed using HMAC /MD5 for mutual authentication of all management data packets. Alternatively, other protocols such as HMAC/SHA-1 are used for verifying data integrity. Less preferably, MD5 or SHA-1 are used absent HMAC. It is evident that verification of data integrity of all management traffic increases security, increases reliability by reducing errors in network management and permits an effective logging of network management operations. Further verifying network management through the use of certificates and network management policy through the use of attribute certificates results in significant flexibility and security.

In order to maintain a complex secured virtual private network comprising a plurality of sub-networks, information relating to each sub-network is required. The information is then used to determine a security gateway to which a request is to be directed in order to reach a desired destination. The information allows for a request to pass through an unsecured number of times in order to reach an associated destination

resource. Further, the information is indicative of information provided by the gateway for use in authentication. In an embodiment, a static map contains a list of resources and for each resource an associated gateway, an associated method of communication such as tunneling, and a distinguishing name. The distinguishing name is indicative of information provided to the requesting system to authenticate the gateway.

Upon issuing a request, a requesting system searches the static map to determine a destination gateway. Communication therewith is initiated via the associated communication method and information is received from the gateway. When the information is as indicated by the static map and is authenticated, the communication of the request can proceed. When the authentication fails, the security of the communication is questionable. Referring to Fig. D7, when a request is for transmission from gateway 74 to resource 72, the static map indicates for resource 72 that gateway 74 should transmit the message using tunneling to gateway 76. Gateway 74 and gateway 76 initiate communication and authenticate each other. The message is then secured through encryption and transmitted to the gateway 76 via the Internet. At the gateway 76, the message is decrypted and transmitted over the network. In this fashion, a static map presents a point to point map of communication over an unsecured medium. All resources behind gateway 76 are listed in the static map as requiring a transmission to gateway 76 using tunneling and so forth. The complexity of the network beyond gateway 76 is of little concern to the sub-network C.

In another embodiment in order to maintain a complex virtual network comprising a plurality of sub-networks, information relating to each sub-network is required. The information is then used to route information efficiently throughout the virtual network and to locate resources. In an embodiment of the invention, a data file is created storing a "current" state of a network. The file is updated on a regular basis and contains information relating to resources and workstations connected to the virtual network. The file comprises a static map of the network. The use of such a static map significantly

improves performance over polling or multiple transmission systems by improving communication efficiency and response times. Further, security is increased since data is transmitted to fewer sub-nets. When a sub-net notes a change in resources or active workstations, a new static map for that sub-net is stored and is then transmitted for storage in the file. Each sub-net monitors its resources for changes.

Alternatively, each sub-net maintains a static map of the entire network. When a sub-net notes a resource modification, a new connection, or a terminated connection, the sub-net updates its static map and transmits the updated static map portion for the sub-net to all other sub-nets. Each sub-net thereby maintains an updated static map of the entire network. When a resource is requested, the sub-net on which the request was initiated searches the static map for an appropriate resource to fulfill the request. When found, the request is routed through the network to fulfill the request.

Referring to Fig. D7, an SVPN is shown comprising three separate corporate networks A, B, and C. When a request from workstation 71 in network C is intended for resource 72 in Network B, a common approach to fulfilling this request is to disconnect from network A and connect via the internet to network B; however, a static map of the network indicates that resource 72 is available in the current network configuration by transmitting a request to network A. From network A the request is transmitted to network B and therein resource 72 is located. Should network B be provided with a gateway (shown as 73) to the Internet, an alternative route exists for the request. The use of static maps allows the system to determine a variety of routing choices to take in the event of network failure at a gateway or at another network node. Also, static maps permit selection of a most secure path for routing a request to a resource. These and other advantages are significant over the prior art.

Connection security policies in an SVPN are governed based on a node pair forming a connection. This requires a significant allocation of resources because as the number of potential nodes increases, the number of connection security policies in the

most general case is n^2-n. For ten possible node connections, this results in 90 security level settings for each possible source/destination node pair. When 100 possible node connections exist, this number jumps to 9900. It is preferable to reduce the number of security level settings in order to facilitate network management, reduce memory requirements, and enhance usability of an SVPN. In an embodiment of the invention, a method of determining a security policy based on a particular host and a flexible security system for providing a negotiation between nodes via the host to determine desired connection security policies is implemented. A host is provided with a security level and a plurality of policies for enforcing the security level. Each node seeking to connect to another node via the host provides a certificate, which is authenticated, and the node is authorized. The nodes then "negotiate" a security level through implementation of the host security level and policies. For example, ISAKMP is flexible enough to permit negotiation of security levels and is used for this purpose. The host based security levels are less flexible than connection based security levels, but host based security levels are easier to administer.

A common concern in network security applications is physical intrusion. A person gaining physical access to a network cable or to a gateway circuit board has access to significant amounts of information. Within the network cable, information is encoded to prevent access. Within each computer, the authorized user can view infomration only for that workstation. Commonly in the gateway, a significant amount of unsecured data exists. Opening a gateway and physically probing electrical connections provides access to data transmitted across each connection. According to the invention, all data stored within a gateway system is encrypted. Therefore, only data in transit is discernable when a gateway system is breached unless the encryption key is found. The key and volatile memory are cleared when the gateway system case is compromised. This secures data from physical access attempts. The data within the gateway is lost as is any data in transit to the gateway since, without volatile memory, the gateway is no longer in operation. The network data, however, remains unaffected.

Numerous other embodiments may be envisaged without departing from the spirit and scope of the invention.

Claims

What we claim is:

1. A system for connecting to a secure virtual private network and an unsecure network simultaneously comprising:
first means for communicating with the unsecure network for providing requests to the unsecure network and for receiving data from the unsecure network;
second means for communicating with the secure virtual private network, the means for providing data in a secured format suitable for transmission via the unsecure network to the destination network;
wherein data from each of the two means for communication is provided to a same physical unsecure data network connection.

2. The system of claim 1 wherein data from the second means is provided to the unsecure network by providing the data to the first means for communicating.

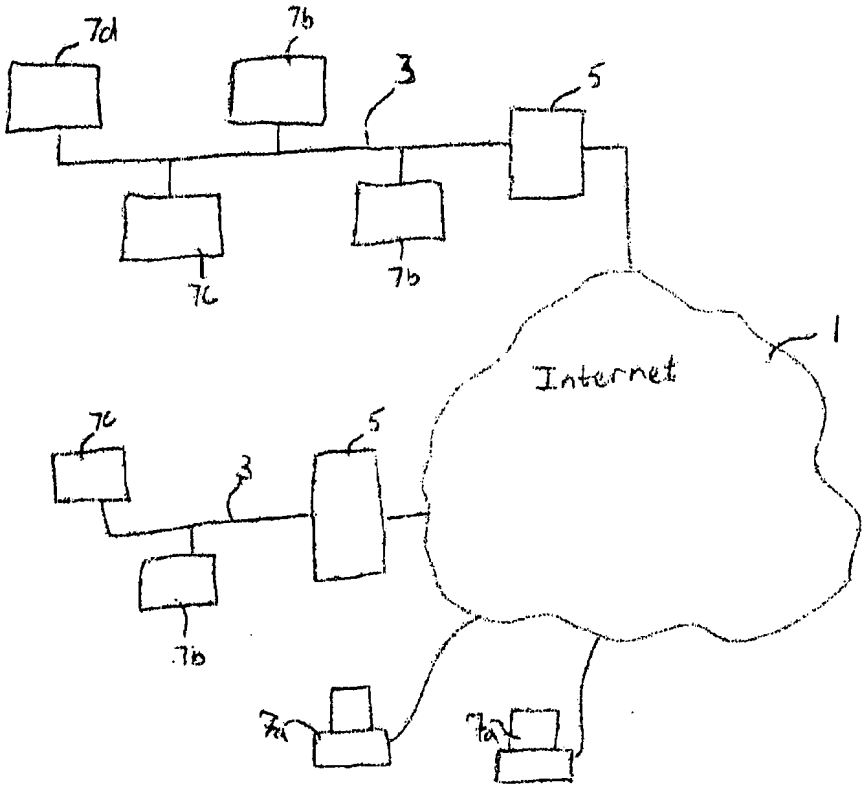


Fig. D1

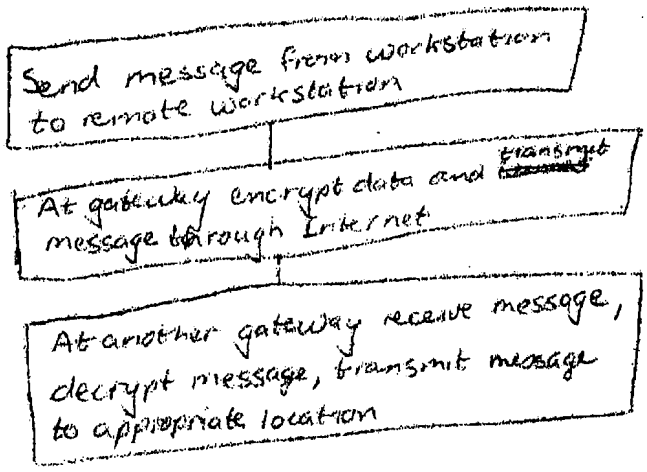

Send message from workstation to remote workstation
At gateway encrypt data and transmit message through Internet
At another gateway receive message, decrypt message, transmit message to appropriate location

Fig. 02

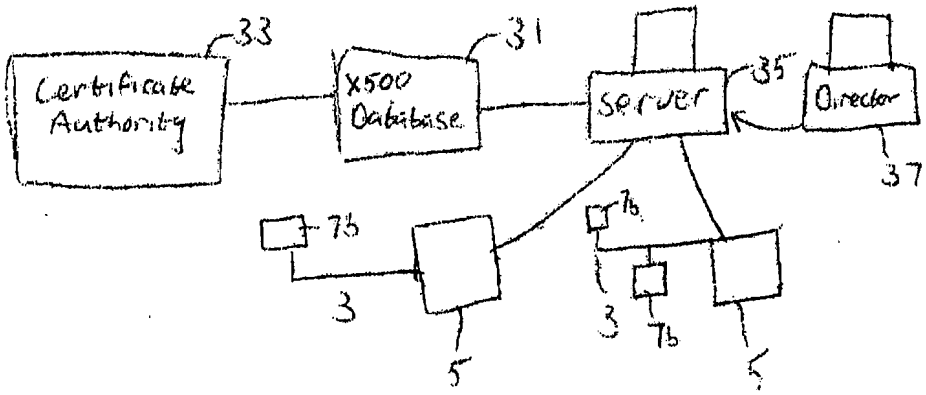

Certificate Authority
33
X500 Database
31
server
35
Director
37
75
3
5
75
3
75
5

Fig. 03

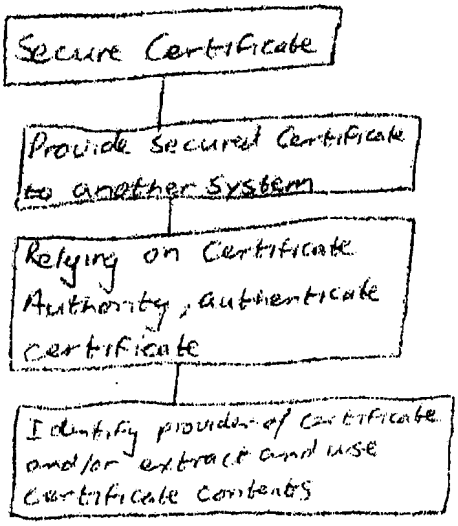
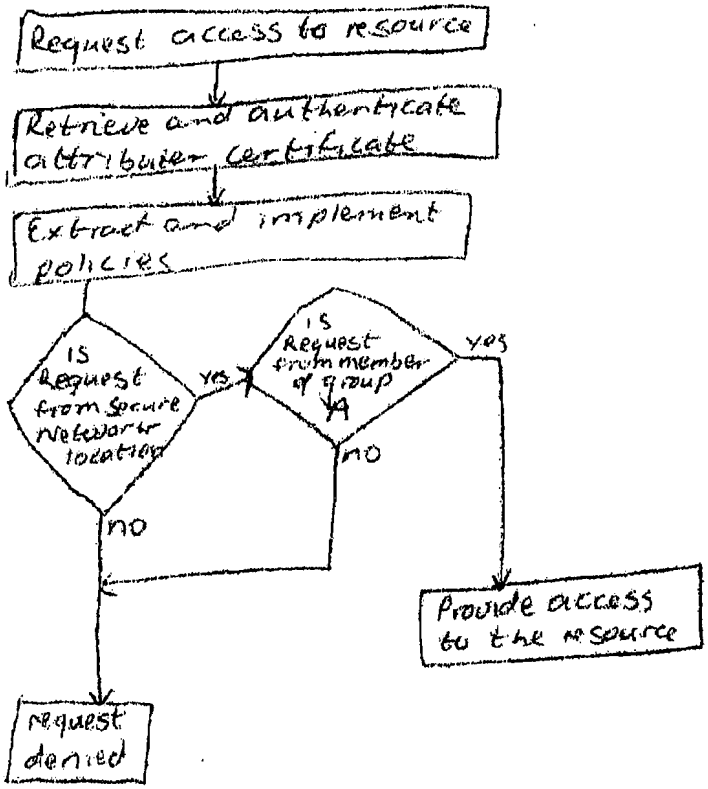

Secure Certificate
Provide secured Certificate to another System
Relying on Certificate Authority, authenticate certificate
Identify provider of certificate and/or extract and use certificate contents

Fig. 04

Fig. 05


Request access to resource
Retrieve and authenticate attribute certificate
Extract and implement policies
IS Request from Secure Network or location
yes
IS Request from member of group
yes
no
no
Provide access to the resource
request denied

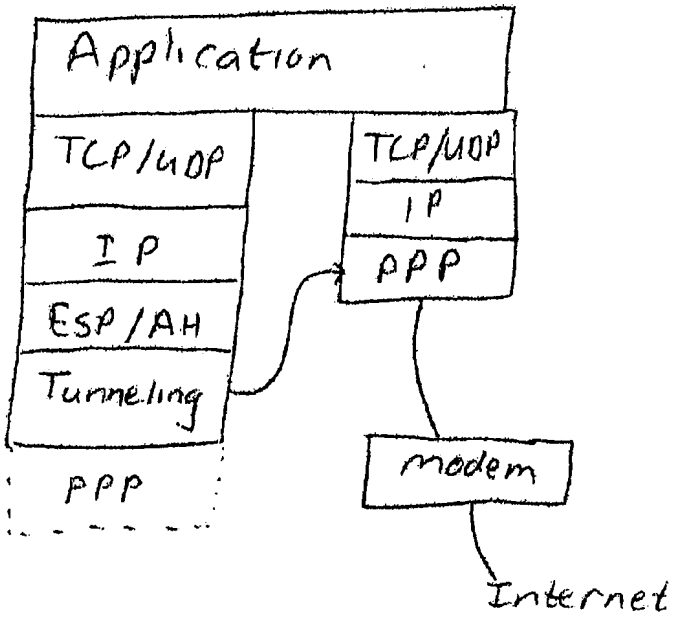
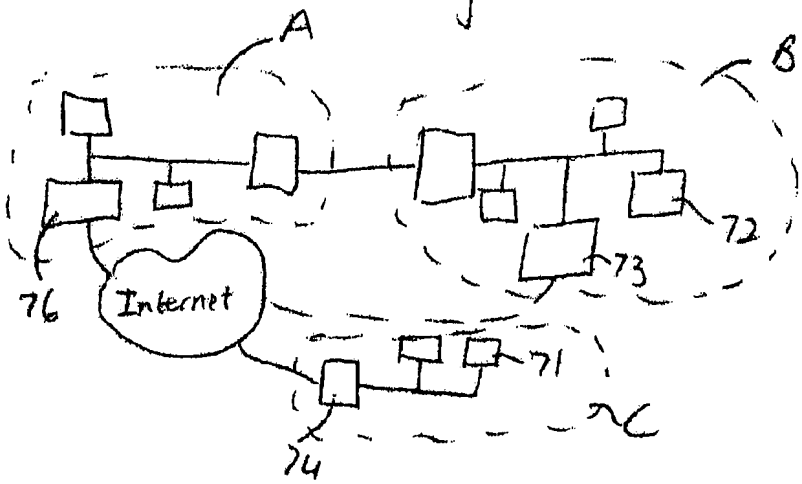

Application
TCP/UDP
IP
ESP/AH
Tunneling
PPP
TCP/UDP
IP
PPP
modem
Internet

Fig. 06

Fig. 07


A
B
72
73
76
Internet
71
74
C